Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for securely storing data for an owner, comprising:

storing the data for the owner consisting at least in part of information relating to the owner's estate by entering the data on a virtual wallet application for the owner, the virtual wallet application having a local aspect residing on a terminal of the owner and a remote aspect residing on a server of a trusted third party coupled to the terminal via a network, ~~and~~ the virtual wallet application also having a virtual executor function, and the virtual wallet application also being configured at least in part for storing data representing at least one of a payment mechanism and electronic funds;

automatically assigning a primary aspect of a secret access device for the virtual wallet application to the owner by the virtual wallet application for accessing the stored data;

automatically escrowing a secondary aspect of the secret access device for the virtual wallet application by the virtual executor function conditioned on the occurrence of an event that renders the owner incapable of acting on the owner's own behalf;

periodically updating the remote aspect of the virtual wallet application with the data stored on the local aspect by a virtual archivist function of the virtual wallet application via the network;

periodically reformatting the data stored on the remote aspect of the virtual wallet application by the virtual archivist function to conform to succeeding methods of accessing the stored data;

receiving verification of the occurrence of the event by the trusted third party from a personal representative of the owner upon the occurrence of the event; and

accessing the stored data by the trusted third party on behalf of the owner's personal representative with the escrowed secret access device.

2. (Canceled)

3. (Previously amended) The method of claim 1, wherein entering the data further comprises entering the data by the owner at the terminal.

4. (Canceled)

5. (Previously amended) The method of claim 1, wherein the terminal further comprises a personal computer.

6. (Canceled)

7. (Previously amended) The method of claim 1, wherein the trusted third party's server further comprises a financial institution server.

8. (Original) The method of claim 7, wherein the financial institution further comprises a bank.

9. (Canceled)

10. (Previously amended) The method of claim 1, wherein the network further comprises a private network.

11. (Previously amended) The method of claim 1, wherein the network further comprises a public network.

12. (Original) The method of claim 11, wherein the public network further comprises the internet.

13-18. (Canceled)

19. (Previously amended) The method of claim 1, wherein entering the data further comprises entering the data on the local aspect of the virtual wallet application residing on the terminal.

20. (Previously amended) The method of claim 1, wherein storing the data further comprises storing at least one category of information by the virtual wallet application for the owner selected from a group of information consisting of identification information, authentication information, certificate information, access key information, PIN number information, credit card account information, debit card information, bank account information, and other personal information.

21. (Canceled)

22. (Previously amended) The method of claim 1, wherein automatically assigning the primary aspect of the secret access device further comprises automatically assigning the primary aspect of the secret access device to the owner at the terminal.

23. (Previously amended) The method of claim 22, wherein automatically assigning the primary aspect of the secret access device further comprises automatically assigning the primary aspect of the secret access device by the remote aspect of the virtual wallet application residing on the server coupled to the terminal.

24. (Original) The method of claim 23, wherein the terminal further comprises a personal computer.

25-27. (Canceled)

28. (Previously amended) The method of claim 23, wherein automatically assigning the primary aspect of the secret access device further comprises automatically sending information about the secret access device to the owner at the terminal coupled to the server over a the network.

29. (Original) The method of claim 28, wherein the network further comprises a private network.

30. (Original) The method of claim 28, wherein the network further comprises a public network.

31. (Original) The method of claim 30, wherein the public network further comprises the internet.

32. (Currently amended) A method for securely storing data for an owner, comprising:

storing the data for the owner consisting at least in part of an electronic copy of the owner's will on a virtual wallet application for the owner, the virtual wallet application having a local aspect residing on a terminal of the owner and a remote aspect residing on a server of a trusted third party coupled to the terminal via a network, ~~and~~ the virtual wallet application also having a virtual executor function, and the virtual wallet application also being configured at least in part for storing data representing at least one of a payment mechanism and electronic funds;

automatically assigning a secret device to the owner for accessing the stored data on the virtual wallet application, wherein automatically assigning the secret device further comprises automatically assigning the secret device by the virtual wallet application with at least two access aspects comprising an owner's access aspect and a trusted third party's access aspect;

automatically escrowing the trusted third party's access aspect by the virtual executor function of the virtual wallet application for the owner conditioned on the occurrence of an event comprising one of the owner's death and the owner's incompetence;

periodically updating the remote aspect of the virtual wallet application with the data stored on the local aspect by a virtual archivist function of the virtual wallet application via the network;

periodically reformatting the data stored on the remote aspect of the virtual wallet application by the virtual archivist function to conform to succeeding methods of accessing the stored data;

receiving verification of the occurrence of the event by the trusted third party from a personal representative of the owner upon the occurrence of the event; and

providing access to the stored data by the trusted third party for the owner's personal representative with the trusted third party's access aspect of the escrowed secret device.

33. (Canceled)

34. (Previously amended) The method of claim 32, wherein automatically assigning the owner's access aspect further comprises automatically sending the owner's access aspect to the owner.

35–37. (Canceled)

38. (Previously amended) The method of claim 32, wherein automatically escrowing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by the virtual executor function of the virtual wallet application on the server of the trusted third party.

39. (Original) The method of claim 38, wherein the trusted third party server further comprises a financial institution computer.

40. (Original) The method of claim 39, wherein the financial institution further comprises a bank.

41. (Currently amended) A method for securely storing data for an owner, comprising:

storing the data for the owner consisting at least in part of information relating to the owner's estate on a virtual wallet application residing at least in part on a trusted third party's server and at least in part on the owner's personal computer coupled to the server via a network, the virtual wallet application also being configured at least in part for storing data representing at least one of a payment mechanism and electronic funds;

automatically assigning a primary aspect of a secret device to the owner for accessing the stored data;

automatically escrowing a secondary aspect of the secret device by a virtual executor function of the virtual wallet application conditioned on the occurrence of an event consisting of one of the owner's death and the owner's incompetence;

~~receiving verification of the occurrence of the event by the virtual executor function from a personal representative of the owner via the trusted third party;~~

periodically updating the part of the virtual wallet application residing on the trusted third party's server with the data stored on the part of the virtual wallet application residing on the owner's personal computer by a virtual archivist function of the virtual wallet application via the network; ~~and~~

periodically reformatting the data stored on the remote aspect of the virtual wallet application by the virtual archivist function to conform to succeeding methods of accessing the stored data;

receiving verification of the occurrence of the event by the virtual executor function from a personal representative of the owner via the trusted third party; and

providing access for the personal representative to the stored data with the escrowed secret device.

42-47. (Canceled)

48. (Previously amended) The method of claim 1, wherein automatically escrowing the secondary aspect of the secret access device further comprises automatically storing at least one type of secret access information selected from a group of secret access information consisting of identification information, authentication information, certificate information, access key information, PIN number information, and password information.

49. (Previously Amended) The method of claim 1, wherein automatically escrowing the secondary aspect of the secret access device further comprises automatically escrowing decryption infrastructure for the owner.

50. (Original) The method of claim 49, wherein automatically escrowing decryption infrastructure further comprises automatically storing at least one decryption infrastructure selected from a group of decryption infrastructure consisting of public key cryptography infrastructure, electronic document infrastructure, digital signature infrastructure, user name infrastructure, password infrastructure, fingerprint scanner infrastructure, and secret key infrastructure.

51-71. (Canceled)

72. (Original) The method of claim 1, further comprising automatically updating technology aspects of the stored data.

73. (Currently Amended) The method of claim 72, wherein automatically updating the technology aspects further comprises automatically updating technology aspects of the data by ~~a~~ the virtual archivist function of the virtual wallet application.

74. (Canceled)

75. (Previously Amended) The method of claim 73, wherein automatically updating the technology aspects further comprises automatically updating the technology

aspects by the virtual archivist function of the virtual wallet application on the server of the trusted third party.

76. (Original) The method of claim 75, wherein the trusted third party further comprises a financial institution.

77. (Original) The method of claim 76, wherein the financial institution further comprises a bank.

78. (Previously Amended) The method of claim 75, wherein automatically updating the technology aspects further comprises automatically updating at least one technology aspect of the data selected from a group of technology aspects consisting of technology related to signing a document, encryption technology, technology related to a key for signing a document, technology related to a document itself, technology related to a certificate revocation list, technology related to a time stamp, and technology related to a notary stamp.

79. (Previously Amended) The method of claim 1, wherein storing the data further comprises receiving the data from another party by the virtual wallet application for the owner.

80. (Original) The method of claim 79, wherein receiving the data further comprises receiving the data by the virtual wallet application for the owner by electronic mail.

81. (Currently Amended) A system for securely storing data for an owner, comprising:

a virtual wallet application having a local aspect residing on a terminal of the owner and a remote aspect residing on a server of a trusted third party coupled to the terminal via a network and capable of storing the data consisting at least in part of information related to the owner's estate for the owner, the virtual wallet application also being configured at least in part for storing data representing at least one of a payment

mechanism and electronic funds, the virtual wallet application also having a virtual archivist function adapted for periodically updating the remote aspect of the virtual wallet application with the data stored on the local aspect via the network, and the virtual archivist function also being adapted for periodically reformatting the data stored on the remote aspect of the virtual wallet application to conform to succeeding methods of accessing the stored data;

wherein the virtual wallet application is adapted for automatically assigning a primary aspect of a secret access device for the virtual wallet application to the owner for accessing the stored data;

a virtual executor function of the virtual wallet application preprogrammed for automatically escrowing a secondary aspect of the secret access device for the virtual wallet application conditioned upon the occurrence of an event comprising one of the owner's death and the owner's incompetence, and upon receiving verification of the occurrence of the event via the trusted third party from a personal representative of the owner, for providing access to the stored data with the escrowed secondary aspect of the secret access device for the personal representative of the owner.

82-92. (Canceled)

93. (Currently amended) A method for securely storing data for an owner, comprising:

providing a virtual wallet application having a local aspect residing on a computing device of the owner and a remote aspect residing on a trusted third party's server, the virtual wallet application also being configured at least in part for storing data representing at least one of a payment mechanism and electronic funds;

assigning a primary aspect of a secret access device to the owner by the virtual wallet application for accessing both aspects of the virtual wallet application by the owner via the computing device coupled to the server over a network;

escrowing a secondary aspect of the secret access device by a virtual executor function of the virtual wallet application preprogrammed to utilize the secondary aspect to allow access to the owner's stored data only to an authorized representative of the owner's estate upon verification of an occurrence of a predefined event that renders the owner incapable of acting on the owner's own behalf;

allowing the owner at the computing device to store data consisting at least in part of information relating to the owner's estate on the local aspect of the virtual wallet application;

periodically updating the remote aspect of the virtual wallet application with the data stored on the local aspect by a virtual archivist function of the virtual wallet application via the network;

periodically reformatting the data stored on the remote aspect of the virtual wallet application by the virtual archivist function according to conform to succeeding methods of accessing the stored data; and

if the occurrence of the predefined event is verified, allowing access for the authorized representative of the owner's estate to the owner's stored data by the virtual executor function utilizing the secondary aspect of the secret access device.